Information Dominance and Cybersecurity

ONR Program Code 31

October 2012

At a Glance

What is it?

- The Information Dominance and Cybersecurity program advances the science of security through interdisciplinary research to ensure safe and secure operations in cyberspace despite threats posed by sophisticated adversaries and latent vulnerabilities in information technology.

How does it work?

- The program conducts basic and applied research that is creating capabilities required for deploying, configuring and securing computing and networking infrastructure supporting cyberspace operations. The research effort includes defending information within our cyberspace domains from potential attacks by enhancing the security aspect of information system infrastructure, including software, hardware and network.

What will it accomplish?

- The program paves the way for future secure cyberspace technology by providing a foundation, understanding and capability for building secure, dynamic and resilient computing and networking systems with reduced window of vulnerability.

Point of Contact

Sukarno Mertoguno
sukarno.mertoguno@navy.mil

Cyberspace is an unconstrained interaction space enabled by the convergence of multiple disciplines, technologies and global networks. It is also an emerging battlespace in which the Navy must exercise information dominance—total control of information and knowledge in transit, at rest and in processing—while denying these capabilities to an adversary.

Cybersecurity is an essential component of information dominance in cyberspace, and a major research focus for the Office of Naval Research. The Information Dominance and Cybersecurity program investigates information security issues, starting from the root of most security breaches, with the goal of achieving robustness and correctness of the underlying hardware and software of the system itself, minimizing potential attack surfaces. Interaction among computer processes within the network as well as between users and computers are weak links in cyber security.

The program also addresses this weakness through the trusted networked computer thrust and the secure information management, sharing and interaction thrust. It probes the foundation and methodology for evaluating security properties of cyberspace's protocols and processes to better measure, verify and assess the collective security of cyberspace.

It also explores the methodology and technology for assuring cyber physical information integrity and trust boundary among networked, tightly interacting and cooperating physical and computing devices, as part of the Navy cyber infrastructure.

Looking into the future to a candidate for replacing current underlying cyberspace technology, this program is also investing in quantum information science for computation and communication. The quantum processing thrust promises techniques that potentially offer a more secure system.

Research Challenges and Opportunities:

- Secure software engineering for network-enabled devices
- Securing the host and network architectures
- Automated threat mitigation, graceful degradation, remediation
- Moving target defenses
- Automated information countermeasure
- Metrics for information assurance
- Quantum computing and communication for security